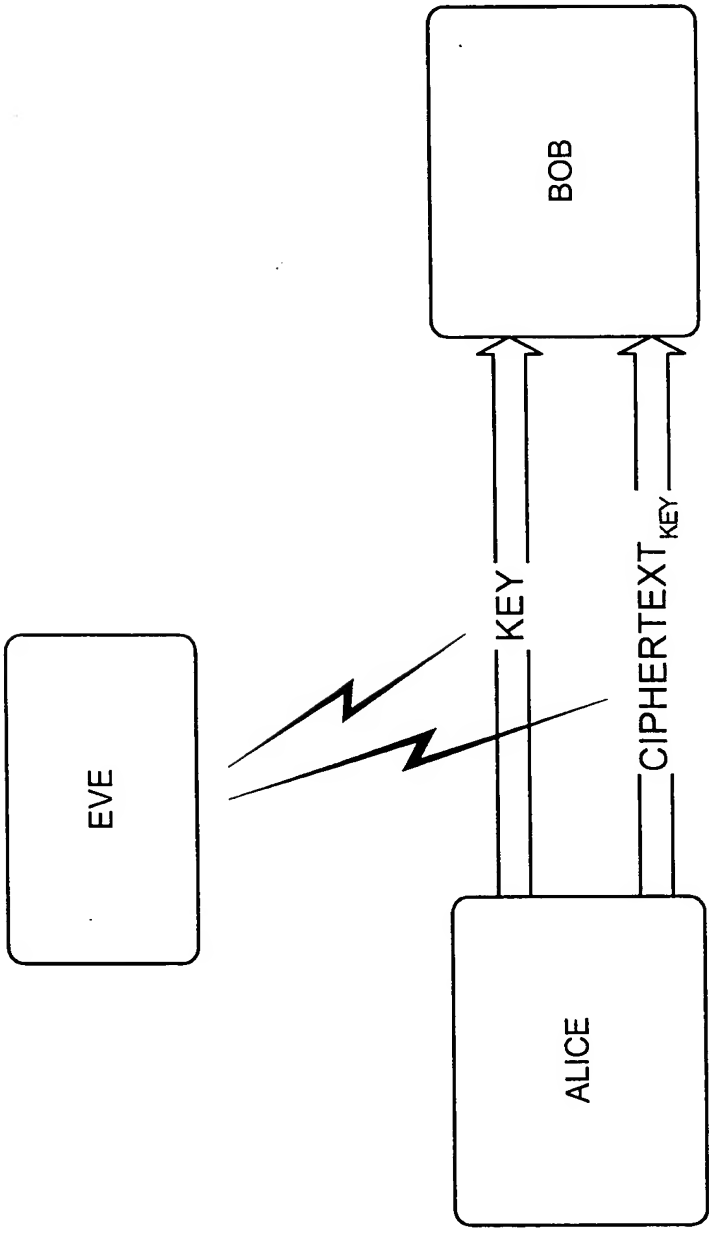

FIG. 1 (PRIOR ART)

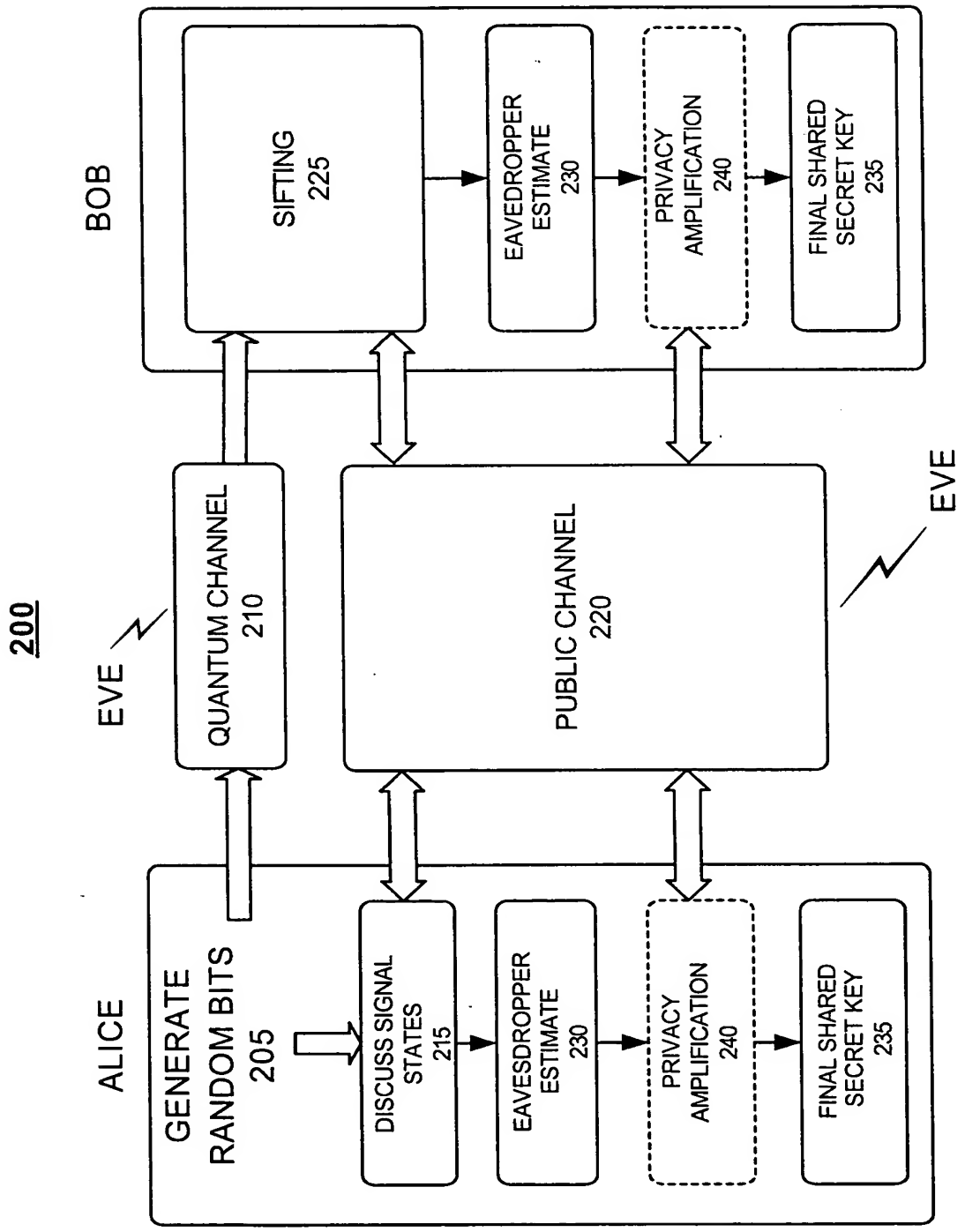

FIG. 2 (PRIOR ART)

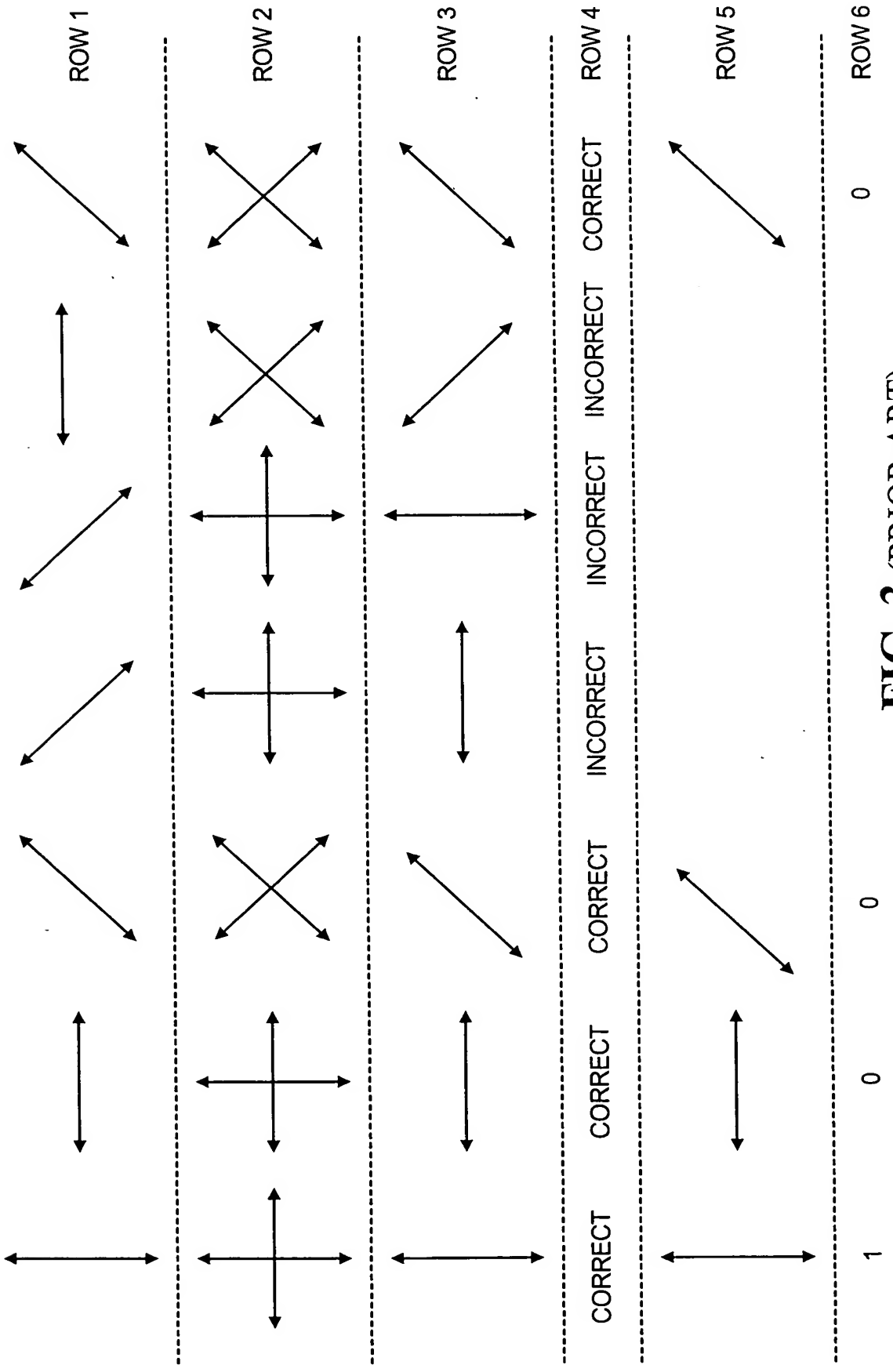

FIG. 3 (PRIOR ART)

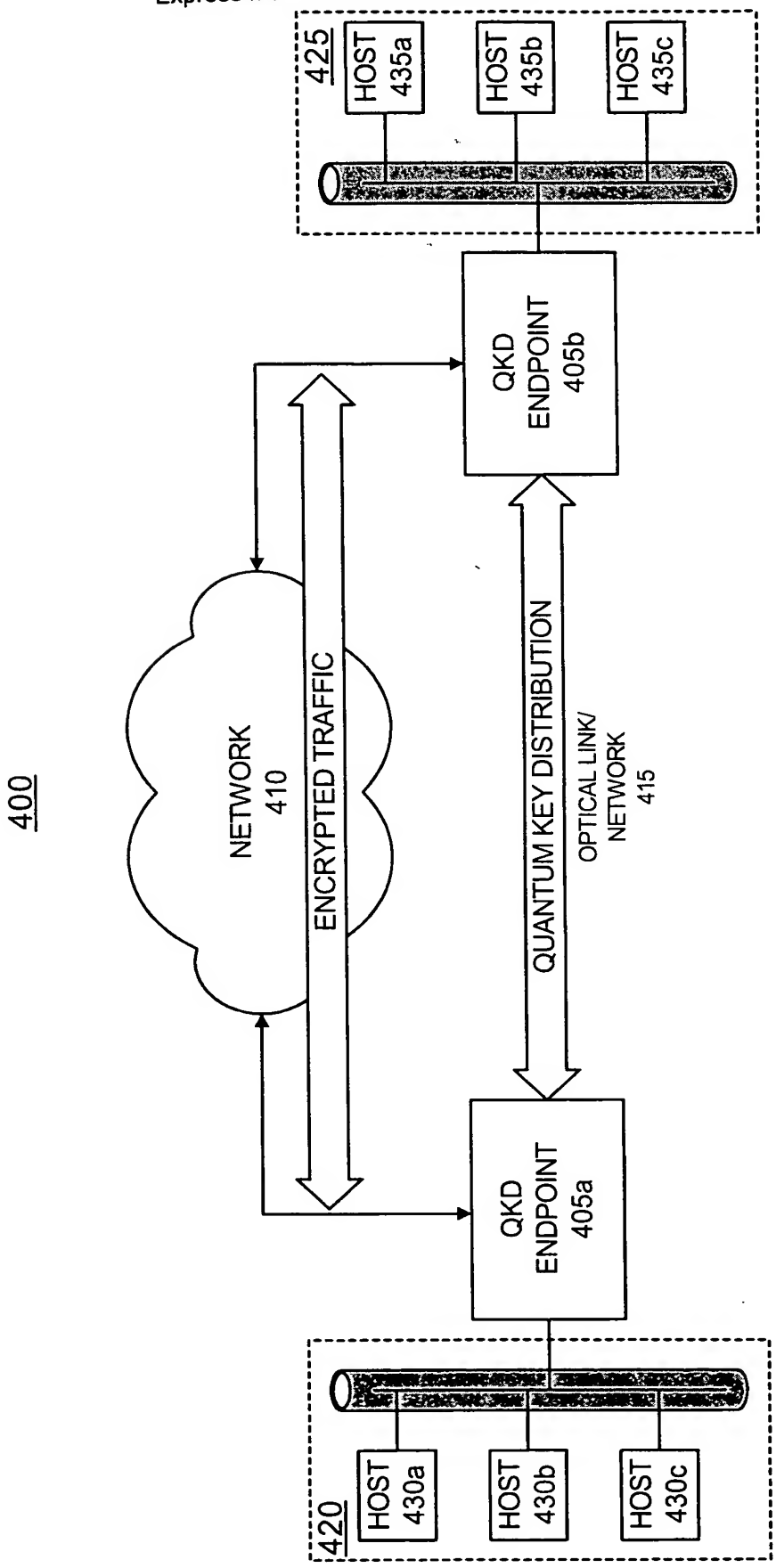
400
425
HOST 435a
HOST 435b
HOST 435c
QKD ENDPOINT 405b
NETWORK 410
ENCRYPTED TRAFFIC
QUANTUM KEY DISTRIBUTION
OPTICAL LINK/ NETWORK 415
QKD ENDPOINT 405a
420
HOST 430a
HOST 430b
HOST 430c

FIG. 4

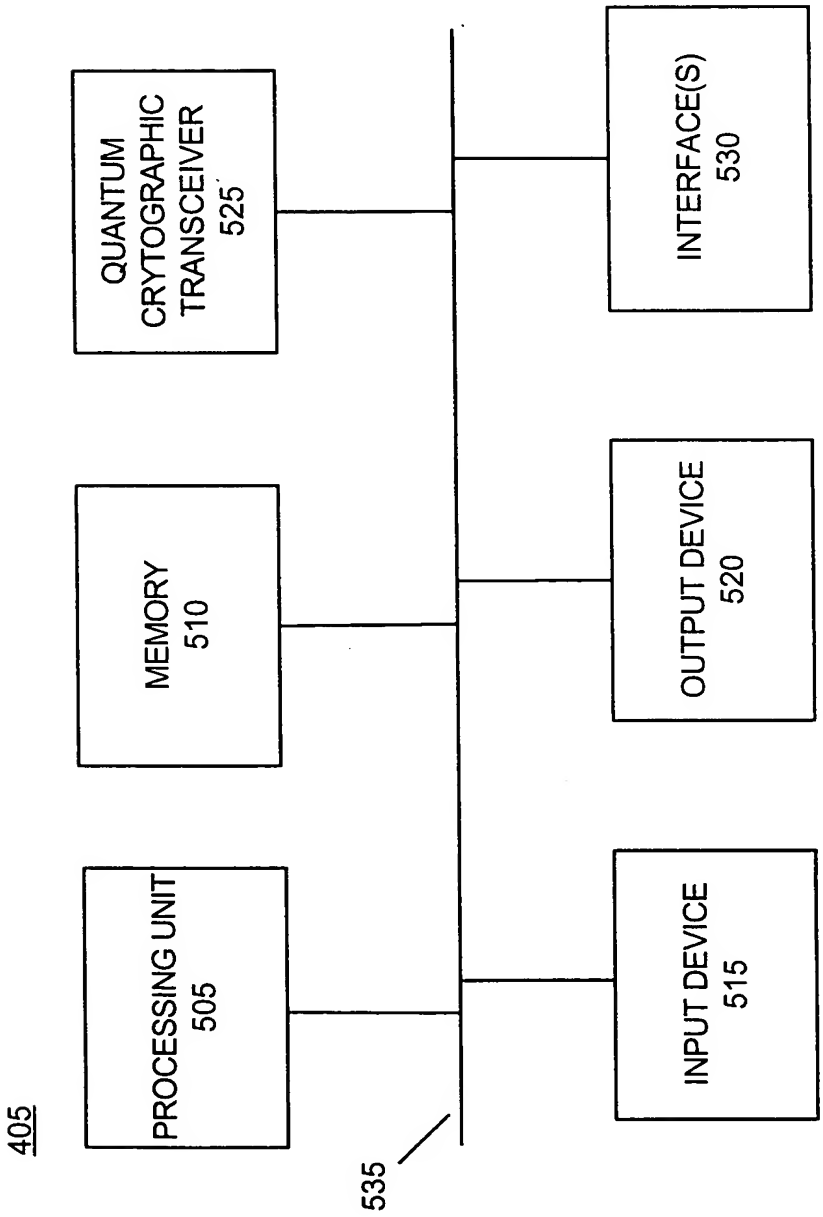
405
PROCESSING UNIT
505
MEMORY
510
QUANTUM
CRYTOGRAPHIC
TRANSCEIVER
525
535
INPUT DEVICE
515
OUTPUT DEVICE
520
INTERFACE(S)
530

FIG. 5

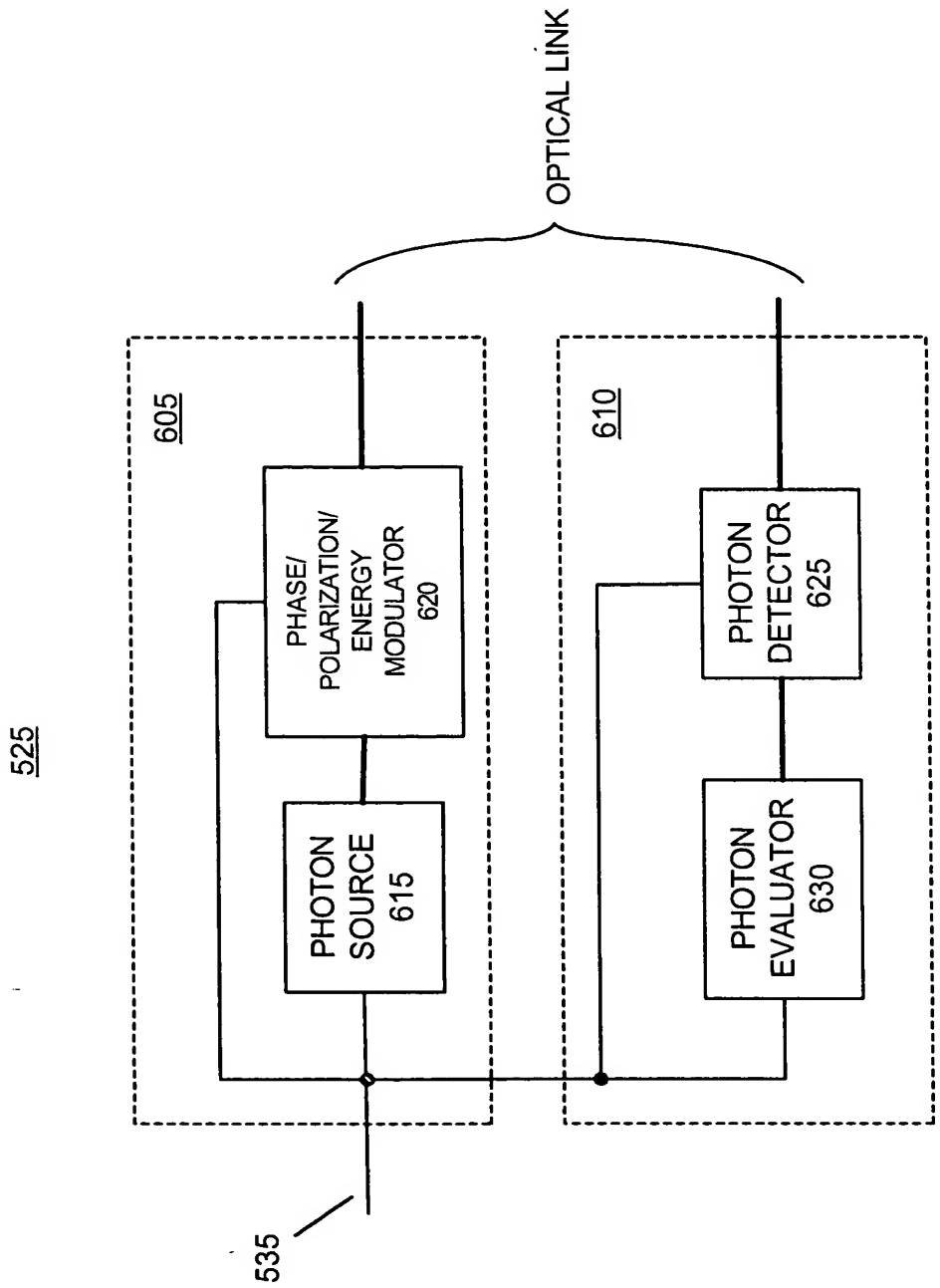
OPTICAL LINK
525
605
610
PHASE/ POLARIZATION/ ENERGY MODULATOR 620
PHOTON SOURCE 615
PHOTON DETECTOR 625
PHOTON EVALUATOR 630
535

FIG. 6

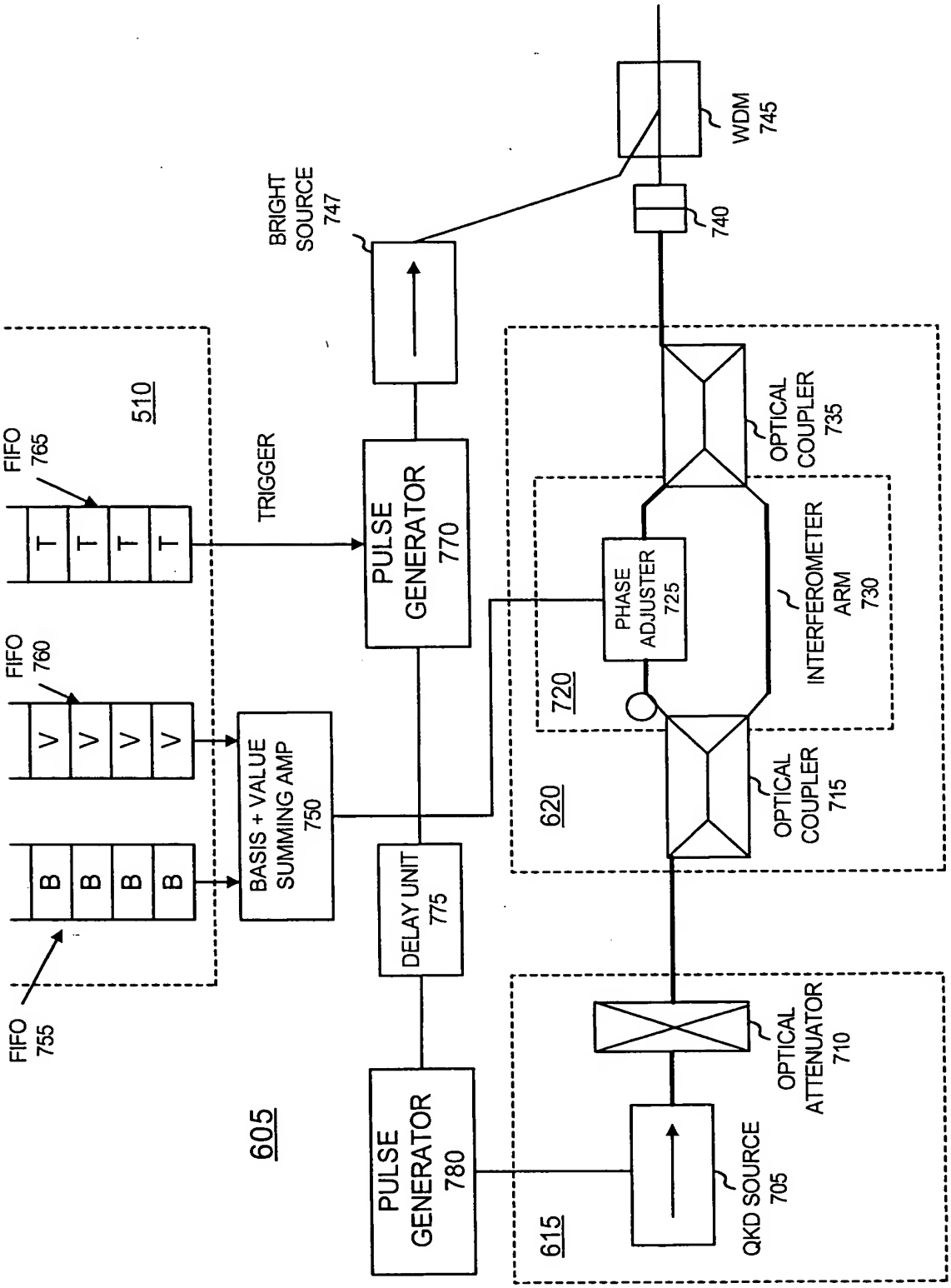
WDM
745
740
BRIGHT SOURCE
747
510
FIFO
765
T
T
T
T
TRIGGER
PULSE GENERATOR
770
OPTICAL COUPLER
735
PHASE ADJUSTER
725
INTERFEROMETER ARM
730
720
FIFO
760
V
V
V
V
BASIS + VALUE SUMMING AMP
750
620
OPTICAL COUPLER
715
B
B
B
B
DELAY UNIT
775
FIFO
755
OPTICAL ATTENUATOR
710
605
PULSE GENERATOR
780
615
QKD SOURCE
705

FIG. 7

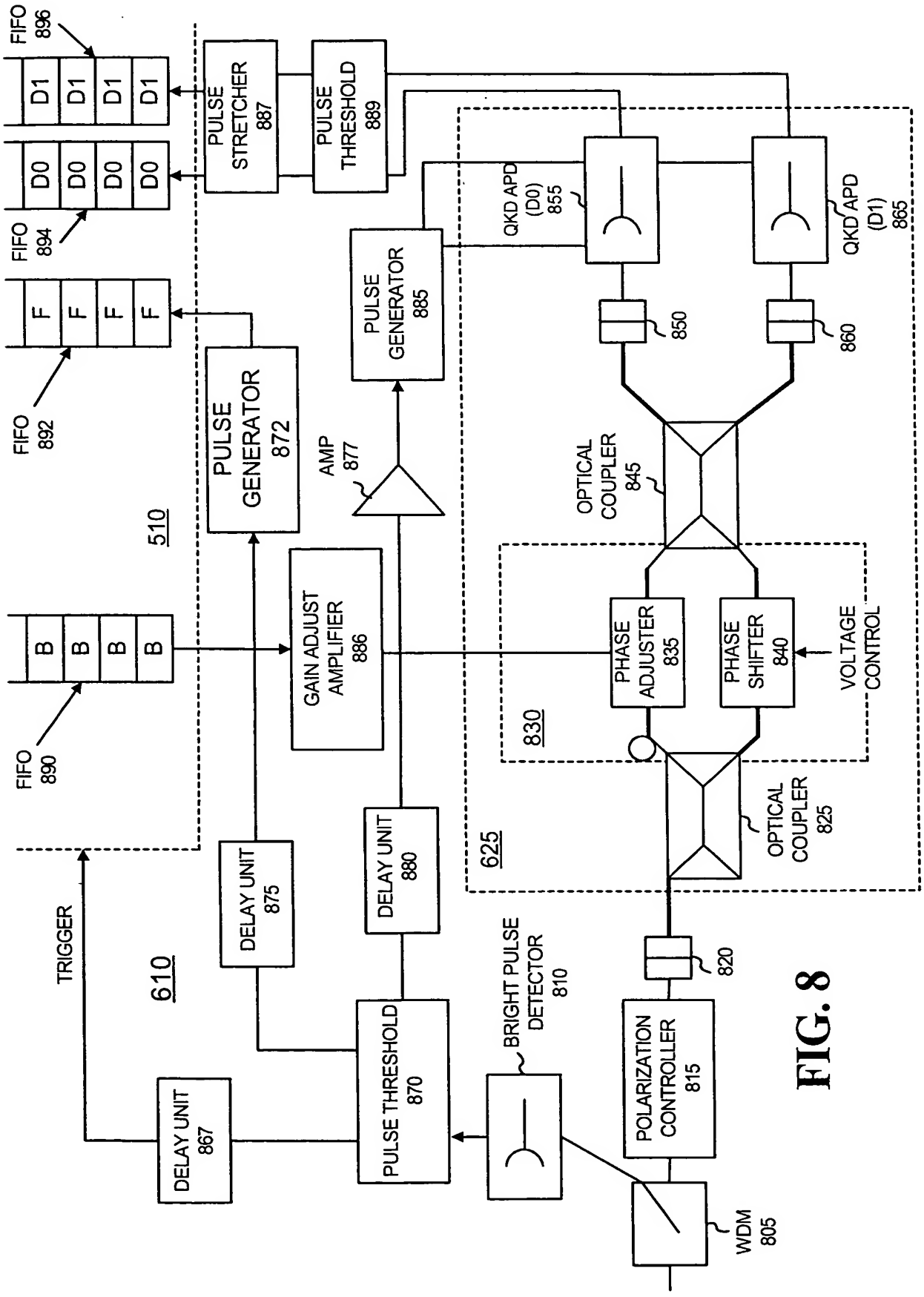
FIFO 896
D1 D1 D1 D1
D0 D0 D0 D0
FIFO 894
F F F F
FIFO 892
B B B B
FIFO 890
PULSE STRETCHER 887
PULSE THRESHOLD 889
PULSE GENERATOR 885
PULSE GENERATOR 872
AMP 877
510
GAIN ADJUST AMPLIFIER 886
DELAY UNIT 875
DELAY UNIT 880
DELAY UNIT 867
TRIGGER
610
PULSE THRESHOLD 870
BRIGHT PULSE DETECTOR 810
QKD APD (D0) 855
QKD APD (D1) 865
850
860
OPTICAL COUPLER 845
PHASE ADJUSTER 835
PHASE SHIFTER 840
VOLTAGE CONTROL
830
625
OPTICAL COUPLER 825
820
POLARIZATION CONTROLLER 815
WDM 805

FIG. 8

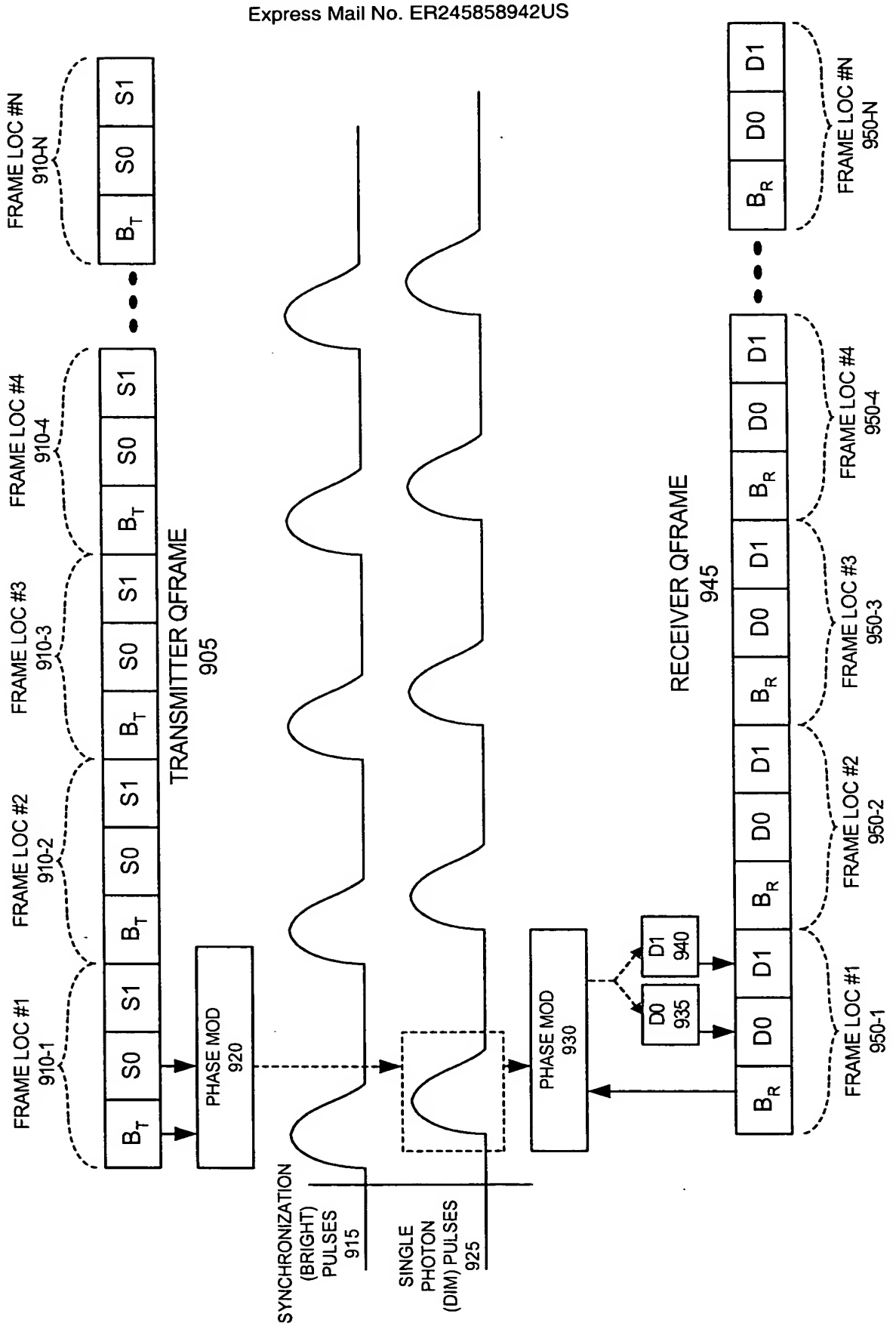
FRAME LOC #1
910-1
FRAME LOC #2
910-2
FRAME LOC #3
910-3
FRAME LOC #4
910-4
FRAME LOC #N
910-N
TRANSMITTER QFRAME
905
PHASE MOD
920
SYNCHRONIZATION (BRIGHT) PULSES
915
SINGLE PHOTON (DIM) PULSES
925
PHASE MOD
930
D0
935
D1
940
RECEIVER QFRAME
945
FRAME LOC #1
950-1
FRAME LOC #2
950-2
FRAME LOC #3
950-3
FRAME LOC #4
950-4
FRAME LOC #N
950-N

FIG. 9

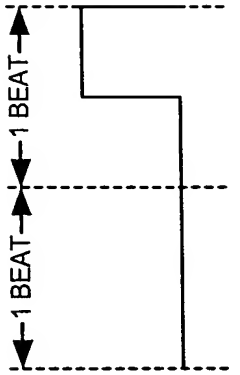

FIG. 10B

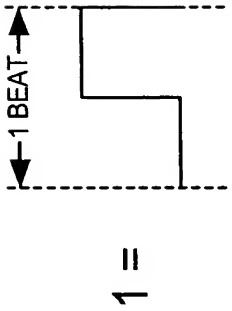

FIG. 10A

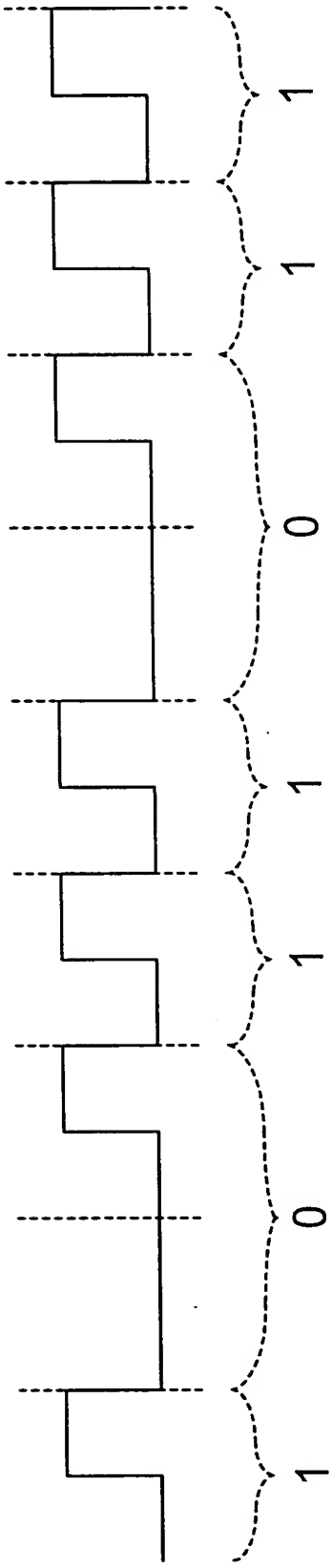

FIG. 10C

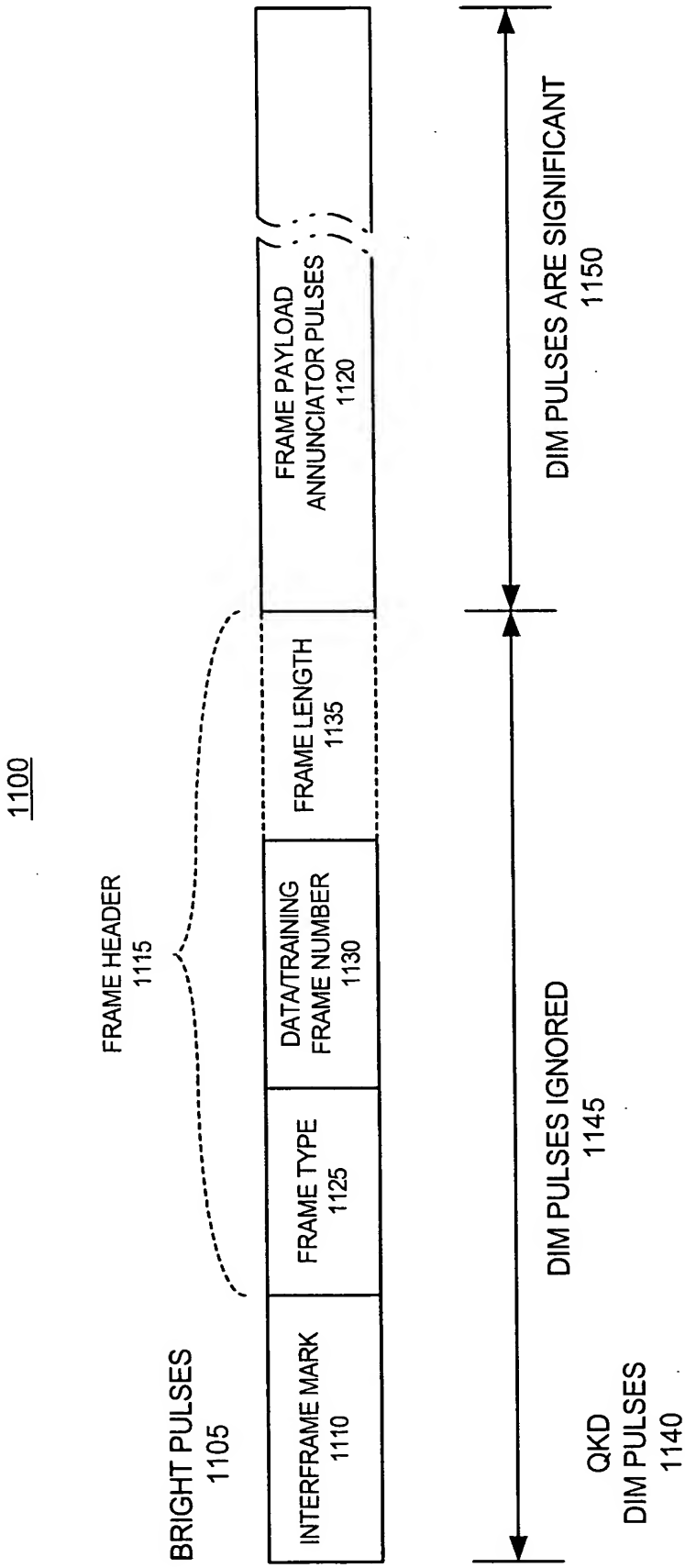
1100
BRIGHT PULSES
1105
FRAME HEADER
1115
INTERFRAME MARK
1110
FRAME TYPE
1125
DATA/TRAINING FRAME NUMBER
1130
FRAME LENGTH
1135
FRAME PAYLOAD ANNUNCIATOR PULSES
1120
QKD DIM PULSES
1140
DIM PULSES IGNORED
1145
DIM PULSES ARE SIGNIFICANT
1150

FIG. 11

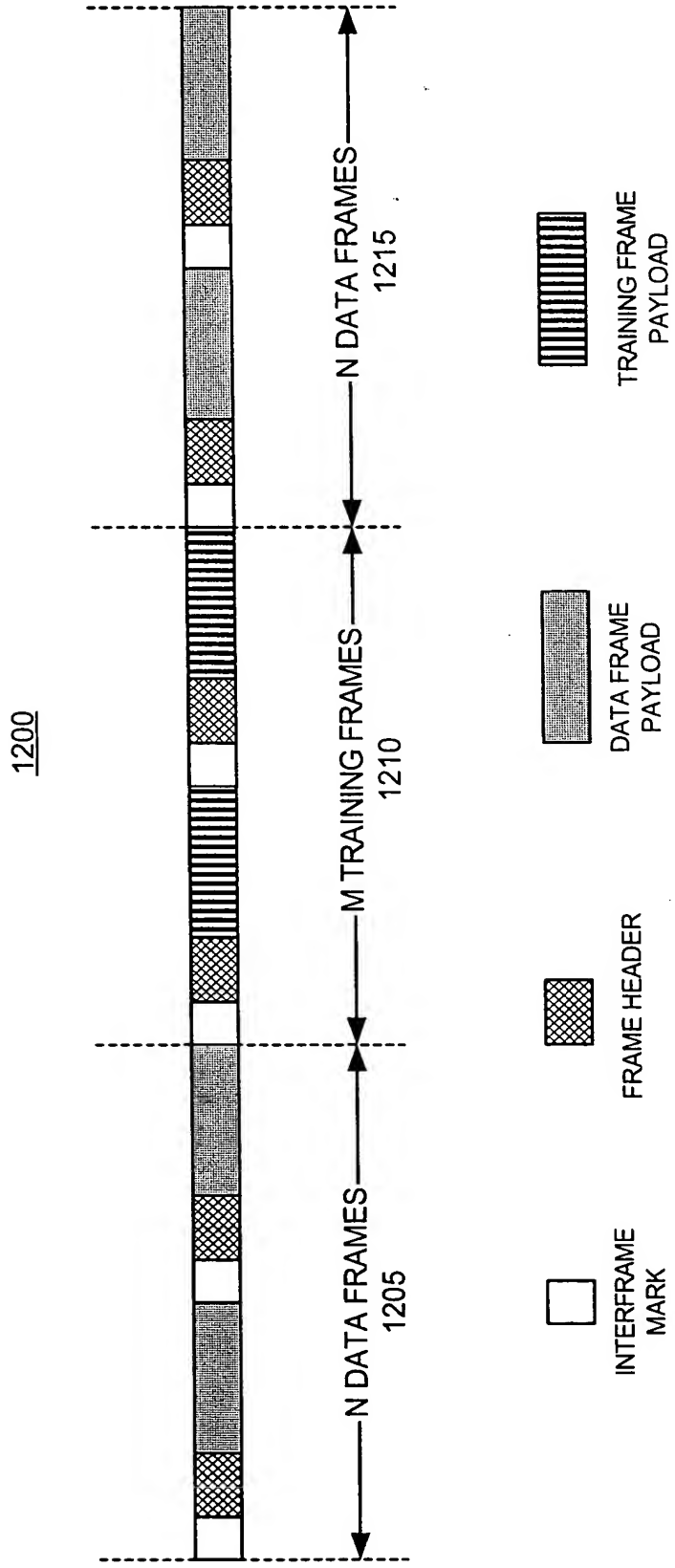
1200
N DATA FRAMES
1205
M TRAINING FRAMES
1210
N DATA FRAMES
1215
INTERFRAME MARK
FRAME HEADER
DATA FRAME PAYLOAD
TRAINING FRAME PAYLOAD

FIG. 12

COUNT TABLE
1300

	ALICE (V, B) 1305	BOB (B_R) 1310	Φ_0 1315	BINNED COUNTS OF TRAINING EVENTS 1320			
				NO D0, D1 HITS 1325	D0 HIT 1330	D1 HIT 1335	D0 & D1 HITS 1340
ROW = 1	(0,0)	0	0				
ROW = 2	(0,0)	1	$3\pi/2$				
ROW = 3	(0,1)	0	$\pi/2$				
ROW = 4	(0,1)	1	0				
ROW = 5	(1,0)	0	π				
ROW = 6	(1,0)	1	$\pi/2$				
ROW = 7	(1,1)	0	$3\pi/2$				
ROW = 8	(1,1)	1	π				
				COLUMN = 1	COLUMN = 2	COLUMN = 3	COLUMN = 4

FIG. 13

JOINT PROBABILITY TABLE
1400

A \ B	EVENT B_0 1425	EVENT B_1 1430	EVENT B_2 1435	EVENT B_3 1440	MARGINAL PROBABILITY 1450
EVENT A_0 1405	$P(A_0 \cap B_0)$	$P(A_0 \cap B_1)$	$P(A_0 \cap B_2)$	$P(A_0 \cap B_3)$	$P(A_0)$
EVENT A_1 1410	$P(A_1 \cap B_0)$	$P(A_1 \cap B_1)$	$P(A_1 \cap B_2)$	$P(A_1 \cap B_3)$	$P(A_1)$
EVENT A_2 1415	$P(A_2 \cap B_0)$	$P(A_2 \cap B_1)$	$P(A_2 \cap B_2)$	$P(A_2 \cap B_3)$	$P(A_2)$
⋮	⋮	⋮	⋮	⋮	⋮
EVENT A_7 1420	$P(A_7 \cap B_0)$	$P(A_7 \cap B_1)$	$P(A_7 \cap B_2)$	$P(A_7 \cap B_3)$	$P(A_7)$
MARGINAL PROBABILITY 1445	$P(B_0)$	$P(B_1)$	$P(B_2)$	$P(B_3)$	$\sum = 1$

FIG. 14

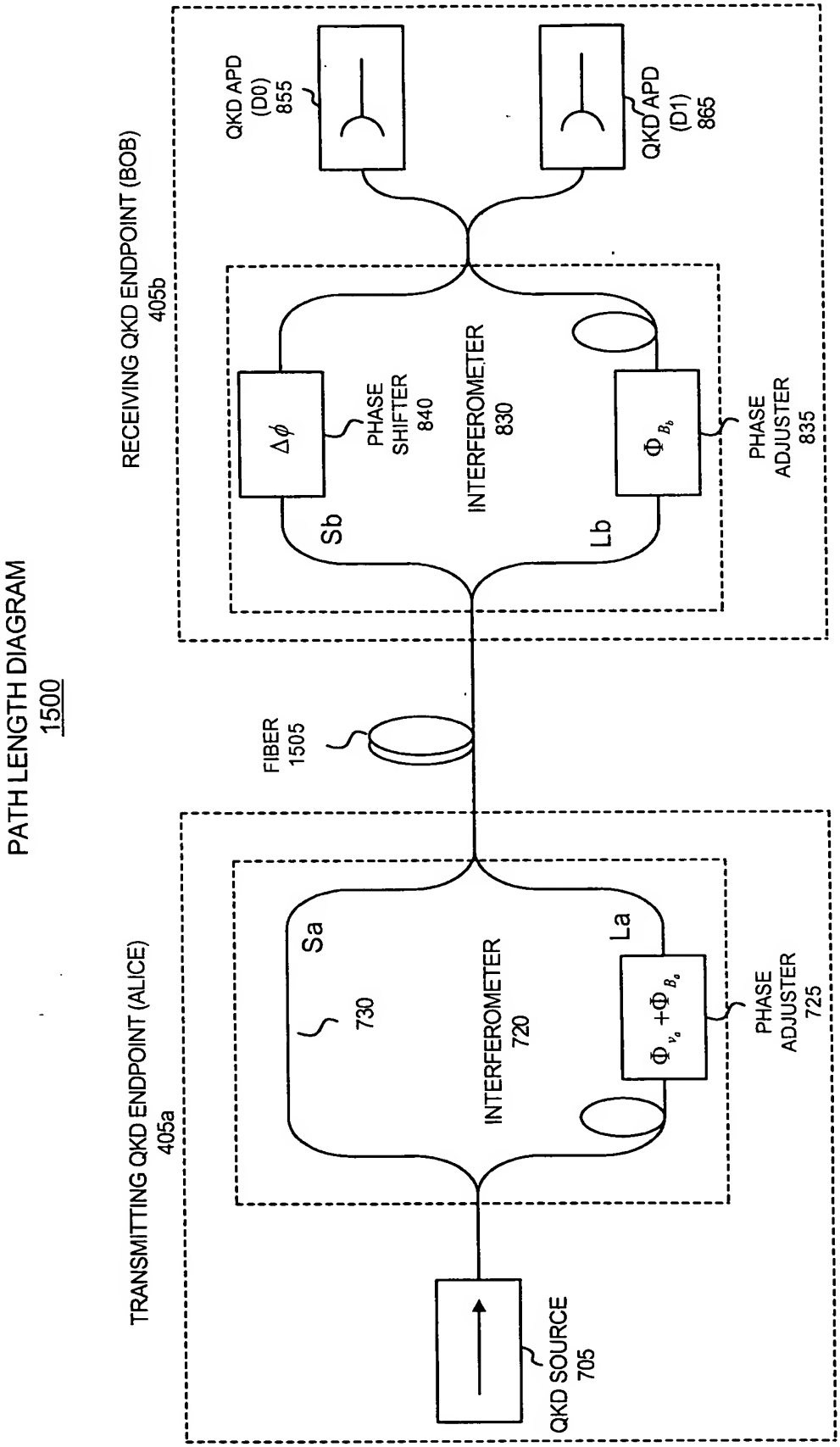
PATH LENGTH DIAGRAM
1500
TRANSMITTING QKD ENDPOINT (ALICE)
405a
QKD SOURCE
705
INTERFEROMETER
720
Sa
730
La
PHASE ADJUSTER
725
FIBER
1505
RECEIVING QKD ENDPOINT (BOB)
405b
INTERFEROMETER
830
Sb
PHASE SHIFTER
840
Lb
PHASE ADJUSTER
835
QKD APD (D0)
855
QKD APD (D1)
865

FIG. 15

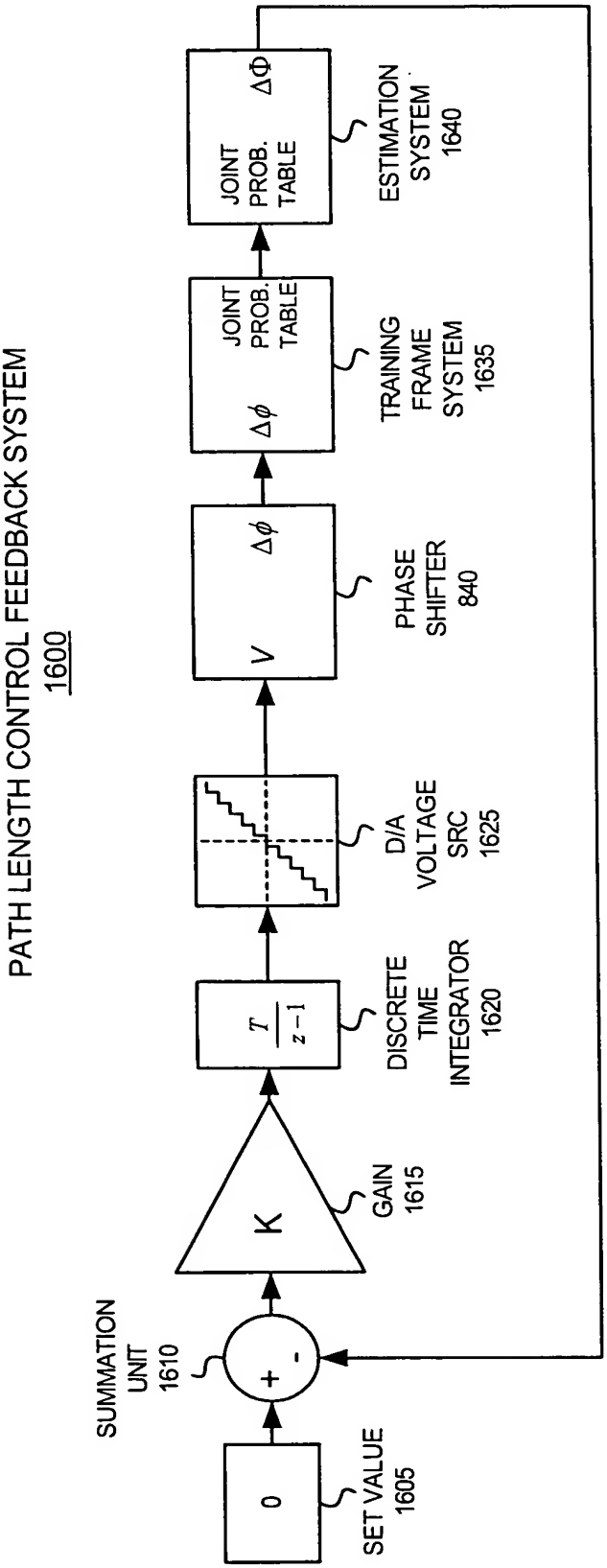
PATH LENGTH CONTROL FEEDBACK SYSTEM
1600
SET VALUE
1605
0
SUMMATION
UNIT
1610
+
-
GAIN
1615
K
DISCRETE
TIME
INTEGRATOR
1620
$\frac{T}{z-1}$
D/A
VOLTAGE
SRC
1625
PHASE
SHIFTER
840
V
$\Delta\phi$
TRAINING
FRAME
SYSTEM
1635
JOINT
PROB.
TABLE
$\Delta\phi$
ESTIMATION
SYSTEM
1640
JOINT
PROB.
TABLE
$\Delta\Phi$

FIG. 16

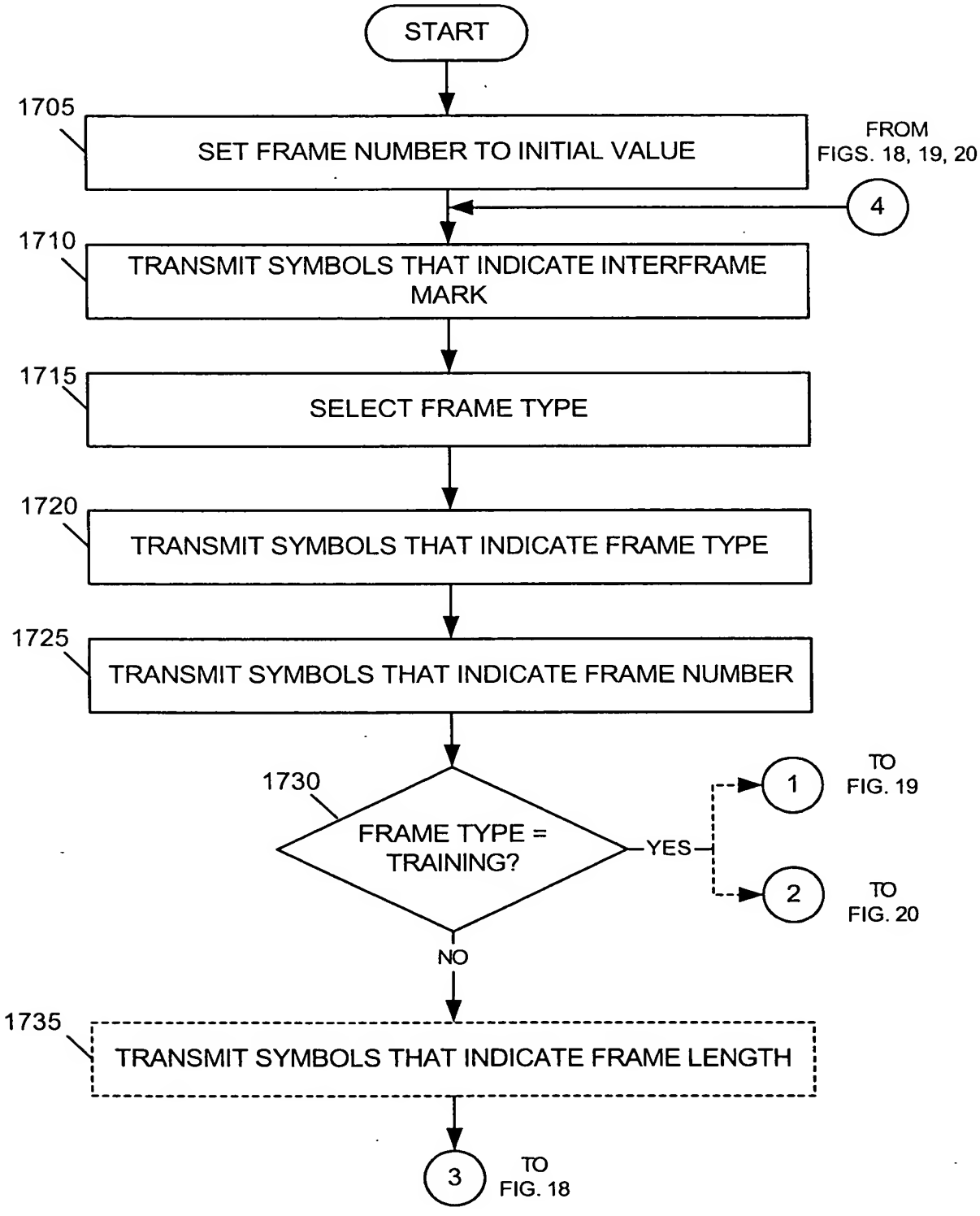
START
1705
SET FRAME NUMBER TO INITIAL VALUE
FROM FIGS. 18, 19, 20
4
1710
TRANSMIT SYMBOLS THAT INDICATE INTERFRAME MARK
1715
SELECT FRAME TYPE
1720
TRANSMIT SYMBOLS THAT INDICATE FRAME TYPE
1725
TRANSMIT SYMBOLS THAT INDICATE FRAME NUMBER
1730
FRAME TYPE = TRAINING?
YES
1
TO FIG. 19
2
TO FIG. 20
NO
1735
TRANSMIT SYMBOLS THAT INDICATE FRAME LENGTH
3
TO FIG. 18

FIG. 17

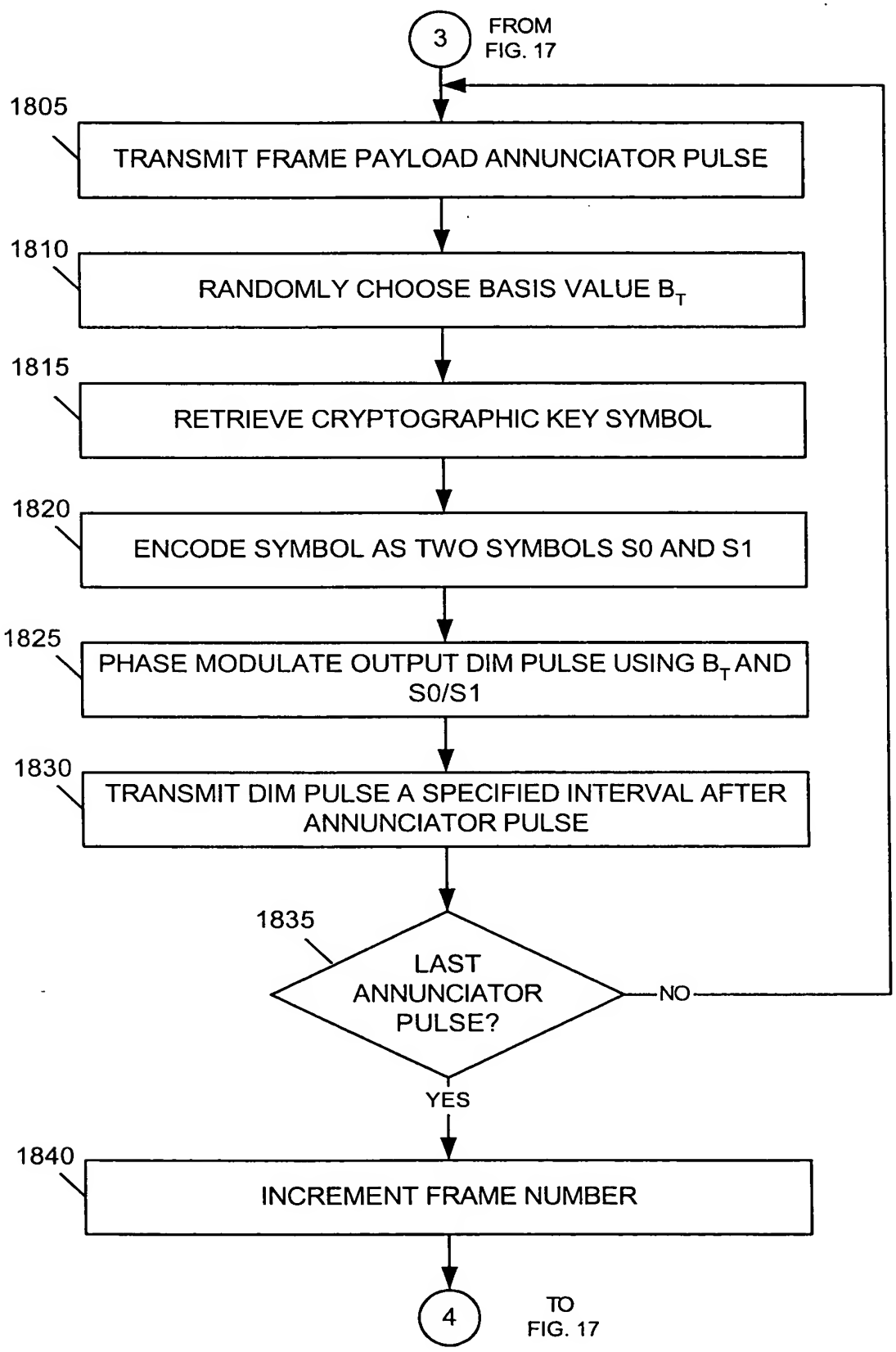
3
FROM FIG. 17
1805
TRANSMIT FRAME PAYLOAD ANNUNCIATOR PULSE
1810
RANDOMLY CHOOSE BASIS VALUE B_T
1815
RETRIEVE CRYPTOGRAPHIC KEY SYMBOL
1820
ENCODE SYMBOL AS TWO SYMBOLS S0 AND S1
1825
PHASE MODULATE OUTPUT DIM PULSE USING B_T AND S0/S1
1830
TRANSMIT DIM PULSE A SPECIFIED INTERVAL AFTER ANNUNCIATOR PULSE
1835
LAST ANNUNCIATOR PULSE?
NO
YES
1840
INCREMENT FRAME NUMBER
4
TO FIG. 17

FIG. 18

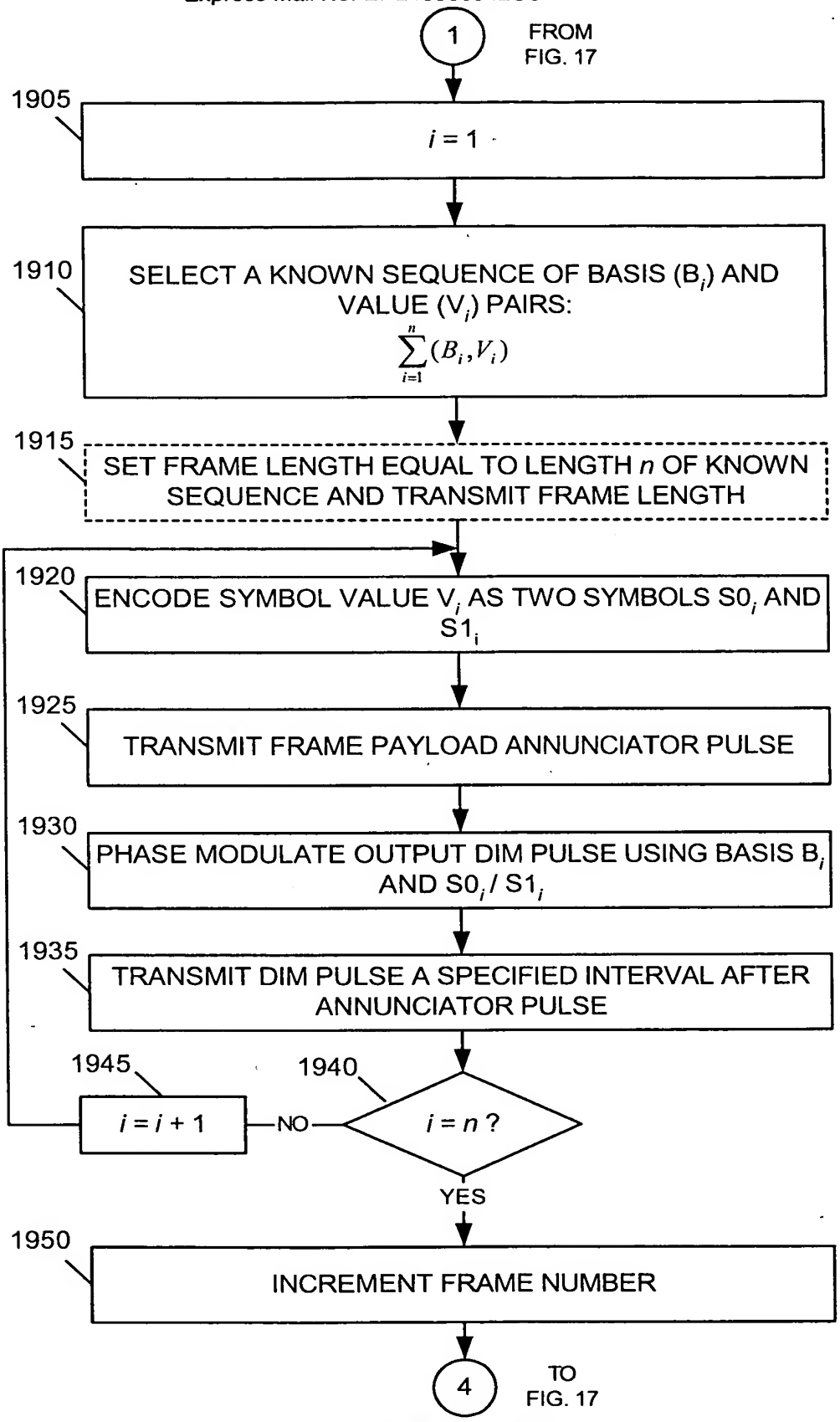
1
FROM FIG. 17
1905
$i = 1$
1910
SELECT A KNOWN SEQUENCE OF BASIS (B_i) AND VALUE (V_i) PAIRS:
$\sum_{i=1}^{n}(B_i, V_i)$
1915
SET FRAME LENGTH EQUAL TO LENGTH n OF KNOWN SEQUENCE AND TRANSMIT FRAME LENGTH
1920
ENCODE SYMBOL VALUE V_i AS TWO SYMBOLS $S0_i$ AND $S1_i$
1925
TRANSMIT FRAME PAYLOAD ANNUNCIATOR PULSE
1930
PHASE MODULATE OUTPUT DIM PULSE USING BASIS B_i AND $S0_i$ / $S1_i$
1935
TRANSMIT DIM PULSE A SPECIFIED INTERVAL AFTER ANNUNCIATOR PULSE
1940
$i = n$?
NO
1945
$i = i + 1$
YES
1950
INCREMENT FRAME NUMBER
4
TO FIG. 17

FIG. 19

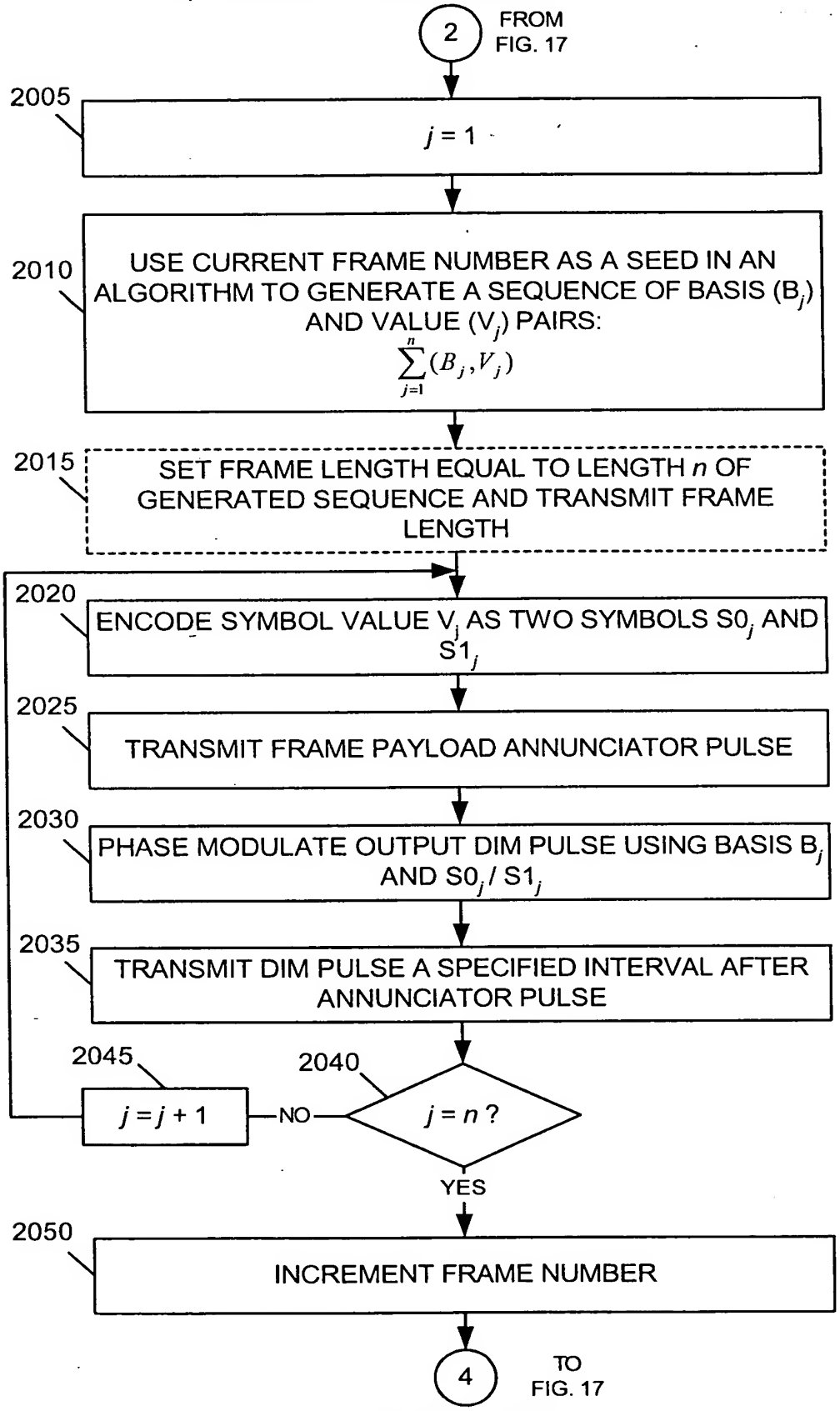
2
FROM FIG. 17
2005
$j = 1$
2010
USE CURRENT FRAME NUMBER AS A SEED IN AN ALGORITHM TO GENERATE A SEQUENCE OF BASIS (B_j) AND VALUE (V_j) PAIRS:
$\sum_{j=1}^{n}(B_j, V_j)$
2015
SET FRAME LENGTH EQUAL TO LENGTH n OF GENERATED SEQUENCE AND TRANSMIT FRAME LENGTH
2020
ENCODE SYMBOL VALUE V_j AS TWO SYMBOLS $S0_j$ AND $S1_j$
2025
TRANSMIT FRAME PAYLOAD ANNUNCIATOR PULSE
2030
PHASE MODULATE OUTPUT DIM PULSE USING BASIS B_j AND $S0_j$ / $S1_j$
2035
TRANSMIT DIM PULSE A SPECIFIED INTERVAL AFTER ANNUNCIATOR PULSE
2040
$j = n$?
NO
2045
$j = j + 1$
YES
2050
INCREMENT FRAME NUMBER
4
TO FIG. 17

FIG. 20

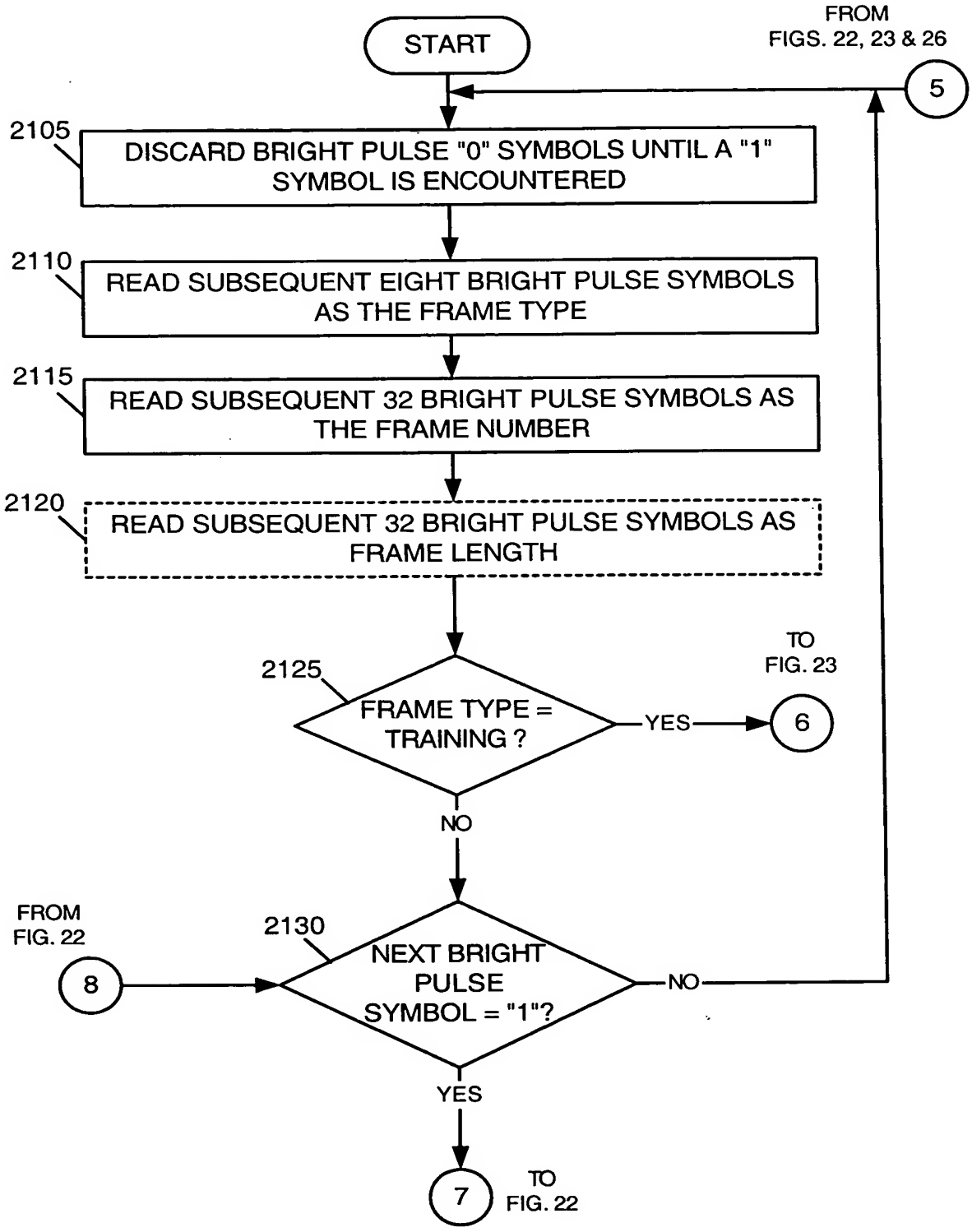
START
FROM FIGS. 22, 23 & 26
5
2105
DISCARD BRIGHT PULSE "0" SYMBOLS UNTIL A "1" SYMBOL IS ENCOUNTERED
2110
READ SUBSEQUENT EIGHT BRIGHT PULSE SYMBOLS AS THE FRAME TYPE
2115
READ SUBSEQUENT 32 BRIGHT PULSE SYMBOLS AS THE FRAME NUMBER
2120
READ SUBSEQUENT 32 BRIGHT PULSE SYMBOLS AS FRAME LENGTH
2125
FRAME TYPE = TRAINING ?
YES
TO FIG. 23
6
NO
FROM FIG. 22
8
2130
NEXT BRIGHT PULSE SYMBOL = "1"?
NO
YES
7
TO FIG. 22

FIG. 21

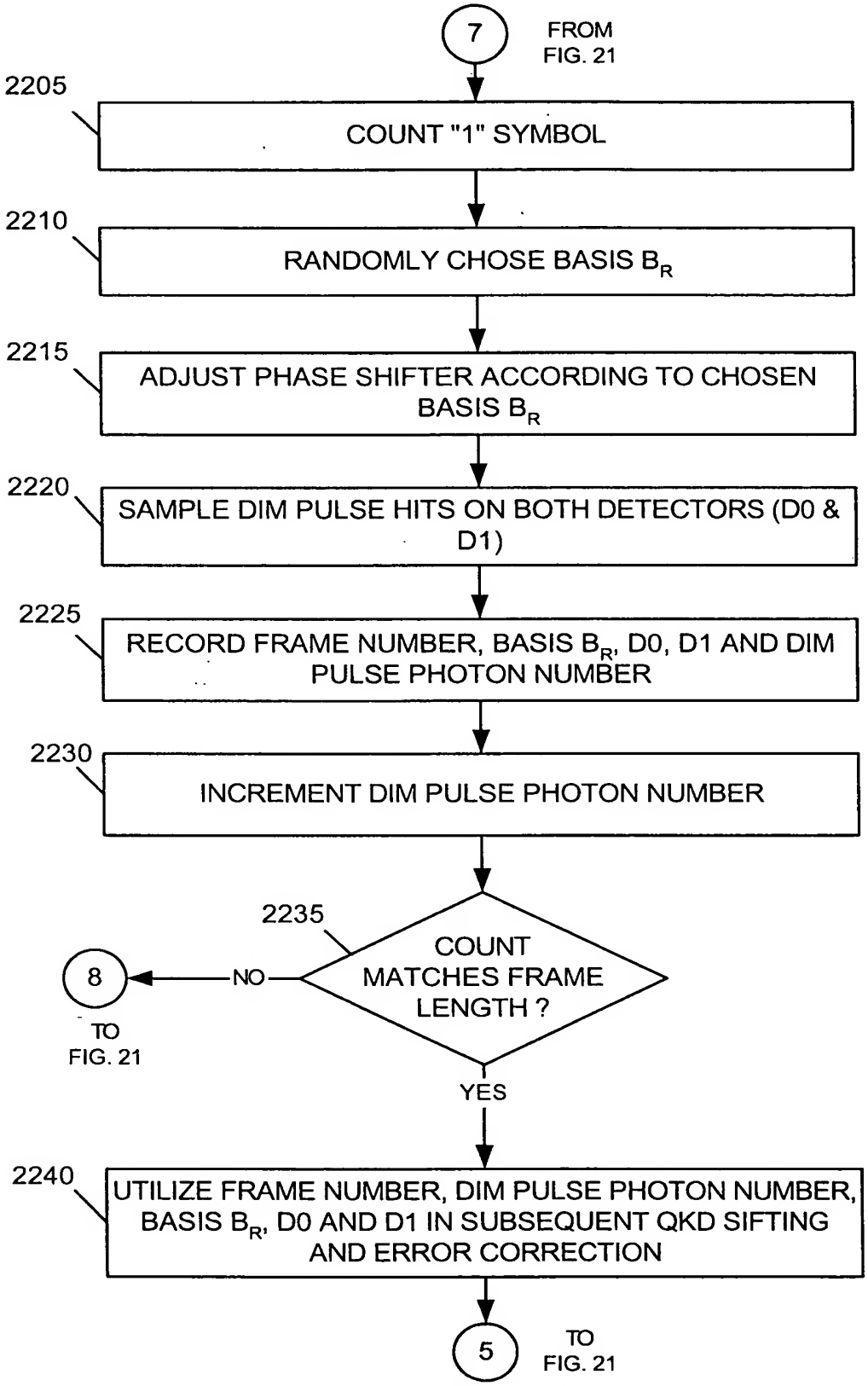
7
FROM FIG. 21
2205
COUNT "1" SYMBOL
2210
RANDOMLY CHOSE BASIS B_R
2215
ADJUST PHASE SHIFTER ACCORDING TO CHOSEN BASIS B_R
2220
SAMPLE DIM PULSE HITS ON BOTH DETECTORS (D0 & D1)
2225
RECORD FRAME NUMBER, BASIS B_R, D0, D1 AND DIM PULSE PHOTON NUMBER
2230
INCREMENT DIM PULSE PHOTON NUMBER
2235
COUNT MATCHES FRAME LENGTH ?
NO
8
TO FIG. 21
YES
2240
UTILIZE FRAME NUMBER, DIM PULSE PHOTON NUMBER, BASIS B_R, D0 AND D1 IN SUBSEQUENT QKD SIFTING AND ERROR CORRECTION
5
TO FIG. 21

FIG. 22

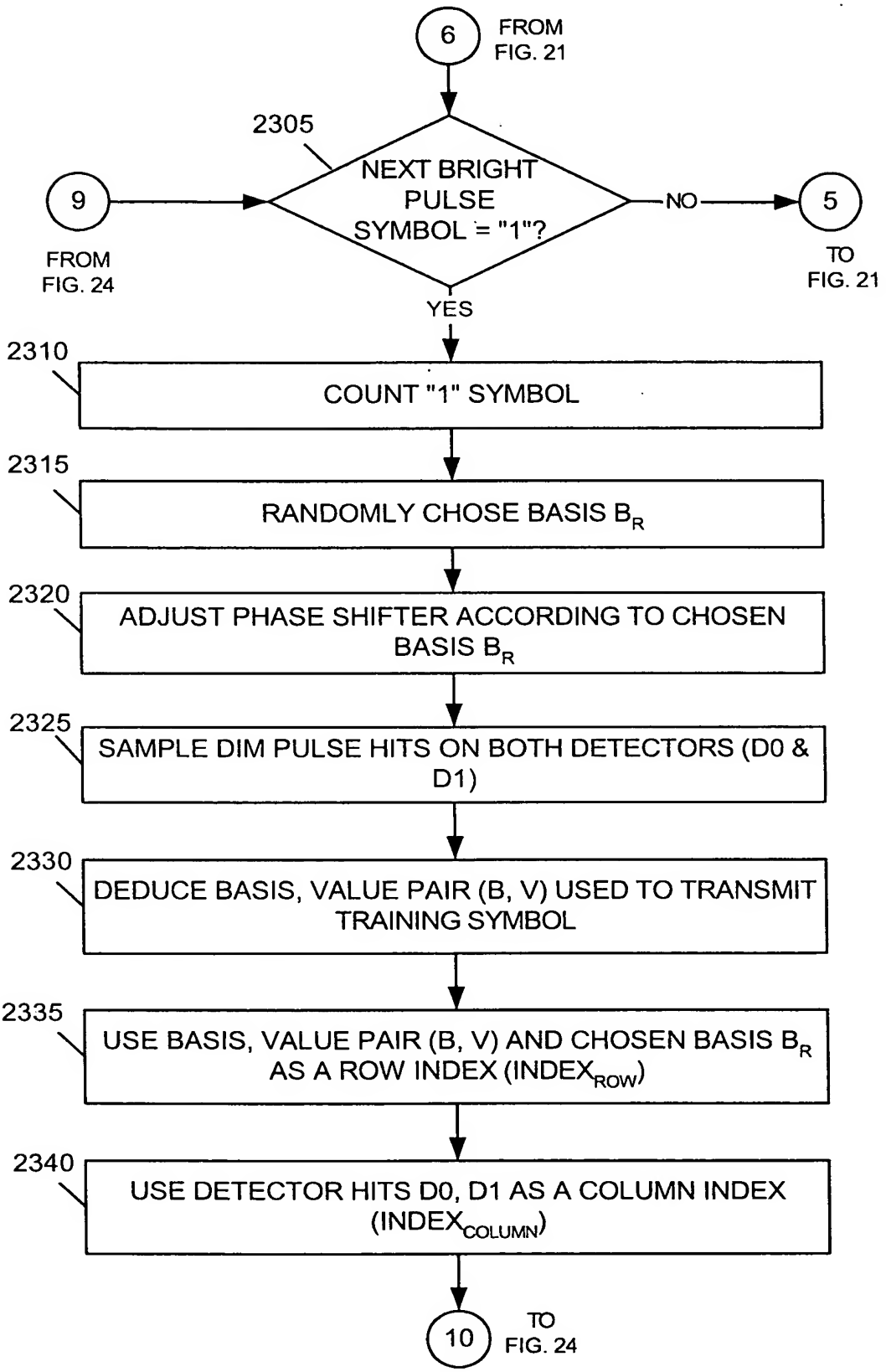
6
FROM FIG. 21
2305
NEXT BRIGHT PULSE SYMBOL = "1"?
NO
5
TO FIG. 21
9
FROM FIG. 24
YES
2310
COUNT "1" SYMBOL
2315
RANDOMLY CHOSE BASIS B_R
2320
ADJUST PHASE SHIFTER ACCORDING TO CHOSEN BASIS B_R
2325
SAMPLE DIM PULSE HITS ON BOTH DETECTORS (D0 & D1)
2330
DEDUCE BASIS, VALUE PAIR (B, V) USED TO TRANSMIT TRAINING SYMBOL
2335
USE BASIS, VALUE PAIR (B, V) AND CHOSEN BASIS B_R AS A ROW INDEX ($INDEX_{ROW}$)
2340
USE DETECTOR HITS D0, D1 AS A COLUMN INDEX ($INDEX_{COLUMN}$)
10
TO FIG. 24

FIG. 23

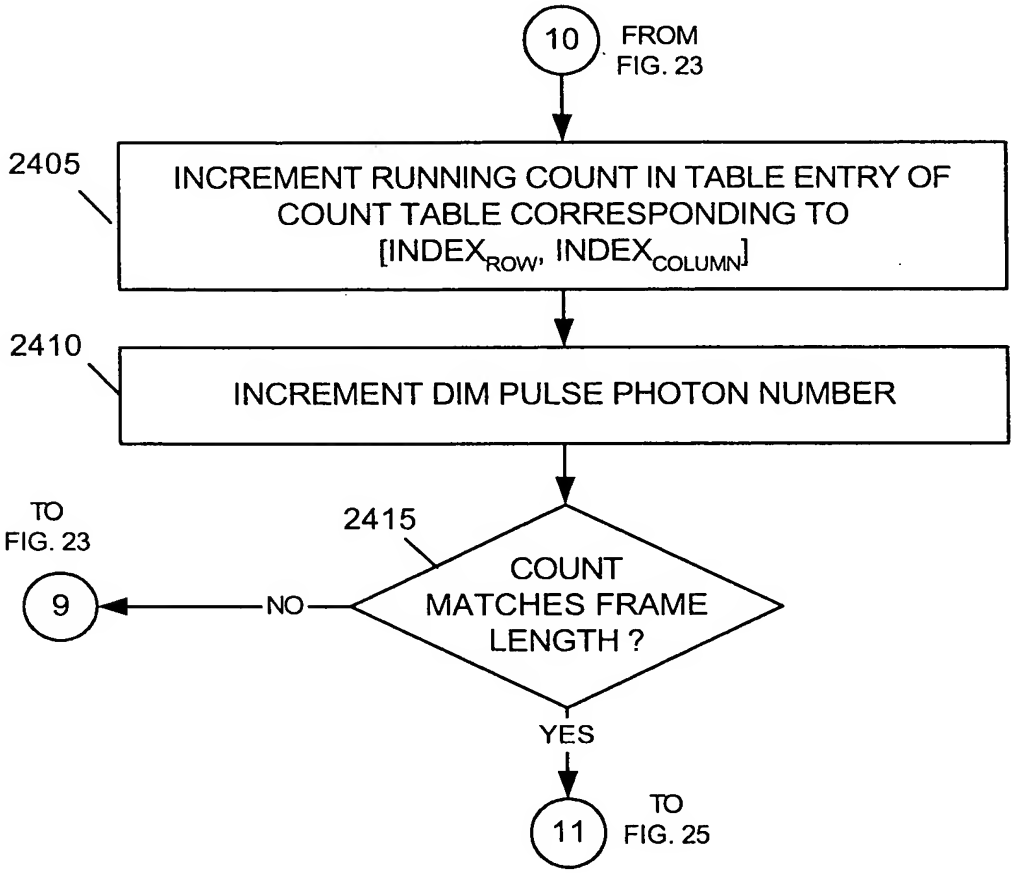
10
FROM FIG. 23
2405
INCREMENT RUNNING COUNT IN TABLE ENTRY OF COUNT TABLE CORRESPONDING TO [INDEX$_{ROW}$, INDEX$_{COLUMN}$]
2410
INCREMENT DIM PULSE PHOTON NUMBER
2415
COUNT MATCHES FRAME LENGTH ?
NO
TO FIG. 23
9
YES
11
TO FIG. 25

FIG. 24

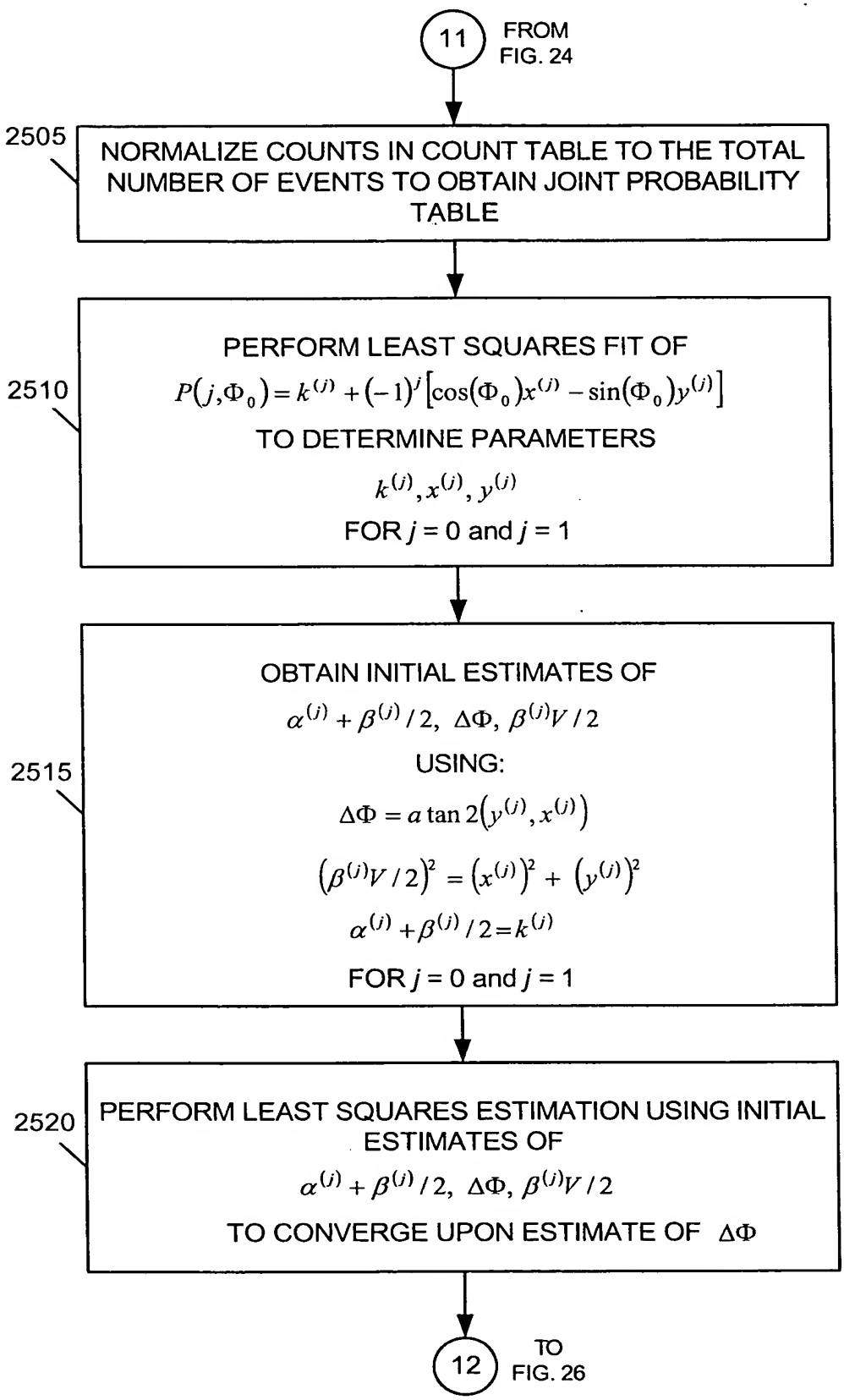
11
FROM FIG. 24
2505
NORMALIZE COUNTS IN COUNT TABLE TO THE TOTAL NUMBER OF EVENTS TO OBTAIN JOINT PROBABILITY TABLE
2510
PERFORM LEAST SQUARES FIT OF
$P(j,\Phi_0) = k^{(j)} + (-1)^j\left[\cos(\Phi_0)x^{(j)} - \sin(\Phi_0)y^{(j)}\right]$
TO DETERMINE PARAMETERS
$k^{(j)}, x^{(j)}, y^{(j)}$
FOR $j = 0$ and $j = 1$
2515
OBTAIN INITIAL ESTIMATES OF
$\alpha^{(j)} + \beta^{(j)}/2,\ \Delta\Phi,\ \beta^{(j)}V/2$
USING:
$\Delta\Phi = a\tan 2\left(y^{(j)}, x^{(j)}\right)$
$\left(\beta^{(j)}V/2\right)^2 = \left(x^{(j)}\right)^2 + \left(y^{(j)}\right)^2$
$\alpha^{(j)} + \beta^{(j)}/2 = k^{(j)}$
FOR $j = 0$ and $j = 1$
2520
PERFORM LEAST SQUARES ESTIMATION USING INITIAL ESTIMATES OF
$\alpha^{(j)} + \beta^{(j)}/2,\ \Delta\Phi,\ \beta^{(j)}V/2$
TO CONVERGE UPON ESTIMATE OF $\Delta\Phi$
12
TO FIG. 26

FIG. 25

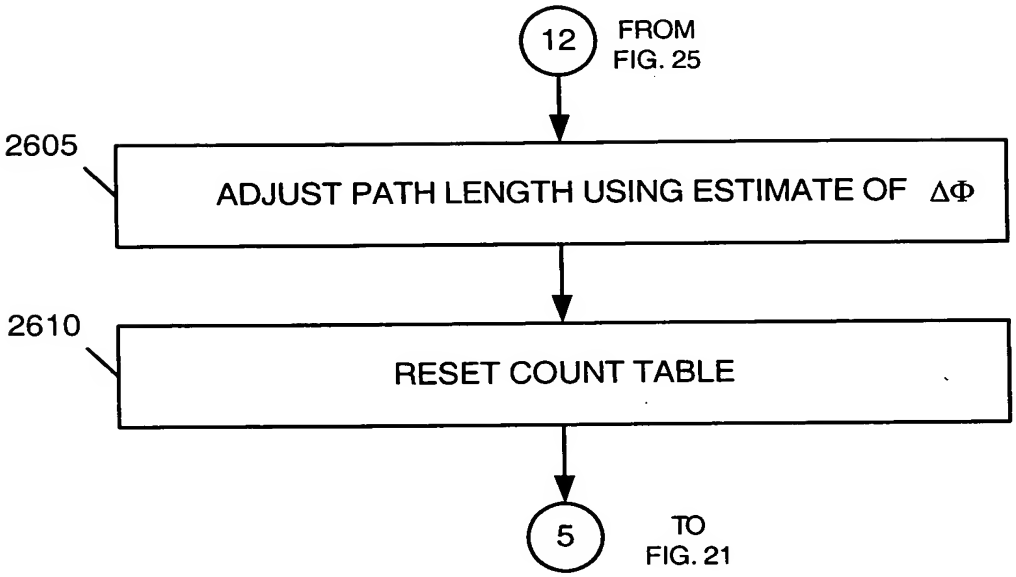
12
FROM FIG. 25
2605
ADJUST PATH LENGTH USING ESTIMATE OF ΔΦ
2610
RESET COUNT TABLE
5
TO FIG. 21

FIG. 26